PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-107083
(43)Date of publication of application : 21.04.1995

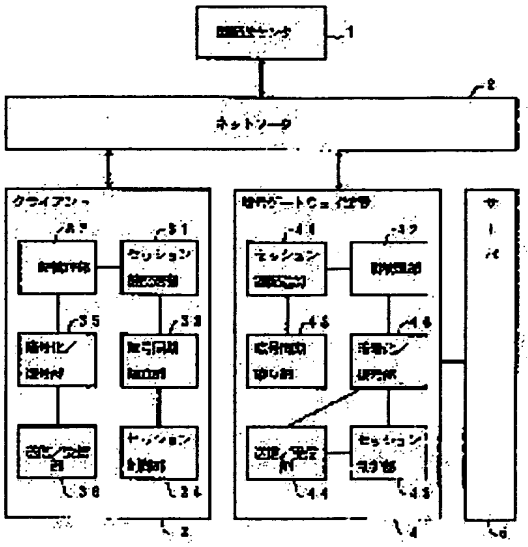
(51)Int.CI. H04L 9/00
H04L 9/10
H04L 9/12
H04L 12/28

(21)Application number : 05-250851
(22)Date of filing : 06.10.1993

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : YAMAGUCHI TOSHIKAZU

(54) CIPHER COMMUNICATION SYSTEM

(57)Abstract:
PURPOSE: To eliminate the need of altering existing application and hardwares and to improve cost effectiveness by sharing a common key among a client, a cipher and a cipher gateway and performing cipher communication using the session key.
CONSTITUTION: The client 3 establishes a session with a cipher gateway device 4 before establishing the session with a server 5 and requests the cipher communication to the device 4. When a communication request is detected, the device 4 receives the session key ciphered by the respective cryptographic keys of the client 3 and the device 4 from a key delivery center 1. Then, the device 4 transmits the session key received from the center 1 to the client 3 and the client 3 receives the session key. The client 3 deciphers the session key by using the cryptographic key of its own and obtains the session key. Thus, the same session key is provided in the client 3 and the device 4. Then, cipher synchronization establishment parts 33 and 34 establish cipher synchronization between the client 3 and the device 4.



LEGAL STATUS

[Date of request for examination] 23.10.1998
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 3263878
[Date of registration] 28.12.2001
[Number of appeal against examiner's decision

(19)日本国特許庁(JP)

(12)特許公報（Ｂ２）

(11)特許番号

特許第３２６３８７８号
（Ｐ３２６３８７８）

(45)発行日　平成14年3月11日(2002.3.11)

(24)登録日　平成13年12月28日(2001.12.28)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ		
Ｈ０４Ｌ	9/08	Ｈ０４Ｌ	9/00	６０１　Ｂ
	12/28		11/00	３１０　Ｚ

請求項の数３　　（全１４頁）

(21)出願番号　特願平5-250851

(22)出願日　平成5年10月6日(1993.10.6)

(65)公開番号　特開平7-107083

(43)公開日　平成7年4月21日(1995.4.21)

審査請求日　平成10年10月23日(1998.10.23)

(73)特許権者　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目3番1号

(72)発明者　山口　利和
東京都千代田区内幸町1丁目1番6号　日本電信電話株式会社内

(74)代理人　100070150
弁理士　伊東　忠彦

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】暗号通信システム

1

(57)【特許請求の範囲】

【請求項１】　ネットワークを介して複数のクライアントならびにサーバが鍵配送センタに接続され、該鍵配送センタが生成したセッション鍵を該ネットワークを介して入手することにより、任意のクライアント・サーバ間でセッションを確立して暗号通信を行う通信システムにおいて、

該サーバと該ネットワークの間に位置し、該クライアントが該サーバとの通信用セッションの確立に先立って出力する暗号通信要求を受信して、該鍵配送センタからセッション鍵を取得し、該クライアントに配送するゲートウェイセッション鍵配送手段と、該鍵配送手段で取得したセッション鍵によりパケットを暗号化または復号する第１の暗号化／復号手段とを含む暗号ゲートウェイ装置と、

2

該サーバとの通信用セッションの確立に先立ち、該暗号ゲートウェイ装置に暗号通信を要求し、該暗号ゲートウェイ装置からセッション鍵を取得するセッション鍵取得手段と、該セッション鍵取得手段により得た該セッション鍵を保持するセッション鍵保持手段と、該暗号ゲートウェイ装置との暗号同期を確立する同期確立手段と、該同期確立手段による同期確立を契機としてサーバとのセッションを確立する第１のセッション確立手段と暗号同期が確立し、かつセッション確立後、パケットを暗号化または復号する第２の暗号化／復号手段とを含むクライアントと、

該クライアント・該サーバ間のセッション確立に先立って、該クライアントからの暗号通信要求に対して、該鍵配送センタから当該セッションで使用するセッション鍵を該暗号ゲートウェイ装置が取得し、該クライアントに

配送し、該クライアント・該ゲートウェイ装置間で共通のセッション鍵を共有することを特徴とする暗号通信システム。

【請求項２】　前記クライアントは、前記サーバとの通信用セッションの確立に先立ち、前記ネットワークを介して前記鍵配送センタからセッション鍵を取得すると共に、前記暗号ゲートウェイ装置に配送するクライアントセッション鍵配送手段を含み、

前記暗号ゲートウェイ装置は、該クライアントからの暗号通信要求と該クライアントセッション鍵配送手段により配送された該セッション鍵を受信するセッション鍵受信手段を含む請求項１記載の暗号通信システム。

【請求項３】　前記クライアントは、前記サーバとの通信用セッションの確立に先立ち、前記暗号ゲートウェイ装置に対して暗号通信を要求するために前記暗号ゲートウェイ装置の特定ポートとセッションを確立する第２のセッション同期確立手段を含み、

前記暗号ゲートウェイ装置は、該第２のセッション同期確立手段による前記クライアントからの特定ポートへのセッション確立を契機として、前記鍵配送センタからセッション鍵を取得し、前記クライアントに配送する第２のゲートウェイセション鍵配送手段を含む請求項１記載の暗号通信システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、暗号通信システムに係り、特に、ネットワークを介して複数のクライアントとサーバが鍵配送センタに接続され、その中の任意のクライアントとサーバが鍵配送センタが生成したセッション鍵を入手し、この鍵を用いてセッションを確立し、共通鍵暗号アルゴリズムを用いてクライアントとサーバ間で暗号通信を行う暗号通信システムに関する。

【０００２】

【従来の技術】図１０は、従来の暗号通信システムの構成を示す。同図に示す従来の暗号通信システムは、ネットワーク２を介して、複数のクライアント3_1～3_3及びサーバ５が鍵配送センタ１に接続され、鍵配送センタ１が生成したセッション鍵をクライアント３またはサーバ５が入手する。

【０００３】図１１は、従来の暗号通信システムを説明するための図である。同図（Ａ）は、鍵配送センタ１にセッション鍵を要求する場合に、クライアント３からアプリケーションプログラムを用いて要求する場合を示し、同図（Ｂ）は、サーバ５からアプリケーションプログラムを用いて要求する場合を示す。このように、クライアント３またはサーバ５がアプリケーションプログラムを用いて通信に使用するセッション鍵を取得する。このセッション鍵をクライアント３とサーバ５間で共有し、以降の通信パケットをこのセッション鍵を用いて暗号化あるいは、復号し、暗号通信を行う。

【０００４】このように、従来の暗号通信システムは、広い地域に分散した事業所等の特定の端末間で暗号通信を行うＬＡＮ等に効果的に利用できるものである。

【０００５】

【発明が解決しようとする課題】しなしながら、上記従来の方式では、暗号通信に先立ち、クライアントあるいはサーバ上で走行するアプリケーションプログラムが鍵配送センタとセッションを確立し、鍵配送センタからセッション鍵を取得し、かつ通信相手のサーバあるいはクライアントのアプリケーションに同じセッション鍵を送信する処理が必要となる。

【０００６】一方、コネクション型のネットワークを介して、クライアント・サーバ間で通信を行う通信プログラムの数は膨大であり、これらを暗号通信対応に変更する場合には、個別にアプリケーションプログラムやクライアントあるいはサーバのハードウェアを改造する必要があり、改造規模や工数が大きくなり、これに伴って、開発費も大きくなるという問題がある。

【０００７】本発明は、上記の点に鑑みなされたもので、上記従来の問題点を解決し、既存のアプリケーションプログラムやハードウェアに影響を与えることなく暗号通信を行うことができる暗号通信システムを提供することを目的とする。

【０００８】

【課題を解決するための手段】図１は、本発明の原理構成図である。

【０００９】本発明は、ネットワーク２を介して複数のクライアント３ならびにサーバ５が鍵配送センタ１に接続され、鍵配送センタ１が生成したセッション鍵をネットワーク２を介して入手することにより、任意のクライアント・サーバ間でセッションを確立して暗号通信を行う通信システムにおいて、サーバ５とネットワーク２の間に位置し、クライアント３がサーバ５との通信用セッションの確立に先立って出力する暗号通信要求を受信して、鍵配送センタ１からセッション鍵を取得し、クライアント３に配送する第１のゲートウェイセッション鍵配送手段１０７と、鍵配送手段１０７で取得したセッション鍵によりパケットを暗号化または復号する第１の暗号化／復号手段１１０とを含む暗号ゲートウェイ装置４と、サーバ５との通信用セッションの確立に先立ち、暗号ゲートウェイ装置４に暗号通信を要求し、暗号ゲートウェイ装置４からセッション鍵を取得するセッション鍵取得手段１０１と、セッション鍵取得手段１０１により得たセッション鍵を保持するセッション鍵保持手段１０２と、暗号ゲートウェイ装置４との暗号同期を確立する同期確立手段１０３と、同期確立手段１０３による同期確立を契機としてサーバ５とのセッションを確立する第１のセッション確立手段１０４と、暗号同期が確立し、かつセッション確立後パケットを暗号化または復号する第２の暗号化／復号手段１１１とを含むクライアント３

と、クライアント・サーバ間のセッション確立に先立って、クライアント３からの暗号通信要求に対して、鍵配送センタ１から当該セッションで使用するセッション鍵を暗号ゲートウェイ装置４が取得し、クライアント３に配送し、クライアント・ゲートウェイ装置間で共通のセッション鍵を共有する。

【００１０】また、本発明のクライアント３は、サーバ５との通信用セッションの確立に先立ち、ネットワーク２を介して鍵配送センタ１からセッション鍵を取得すると共に、暗号ゲートウェイ装置４に配送するクライアントセッション鍵配送手段１０５を含み、暗号ゲートウェイ装置４は、クライアント３からの暗号通信要求とクライアントセッション鍵配送手段１０５から配送されたセッション鍵を受信するセション鍵受信手段１０８を含む。

【００１１】また、本発明のクライアント３は、サーバとの通信用セッションの確立に先立ち、暗号ゲートウェイ装置４に対して暗号通信を要求するために暗号ゲートウェイ装置４の特定ポートとセッションを確立する第２のセッション確立手段１０６を含み、暗号ゲートウェイ装置４は、第２のセション同期確立手段１０６によるクライアント３からの特定ポートへのセッションの確立を契機として、鍵配送センタ１からセッション鍵を取得し、クライアント３に配送する第２のゲートウェイセッション鍵配送手段１０９を含む。

【００１２】

【作用】図２は、本発明のシーケンスの概要を示す図である。

【００１３】本発明の暗号通信システムは、サーバとネットワークの間に位置する暗号ゲートウェイ装置は、クライアント・サーバ間のセッション確立に先立って、クライアントからの暗号通信要求（ステップ１）に対して、鍵配送センタから当該センッションで使用するセッション鍵を取得し（ステップ２）、クライアントに配送する（ステップ３）。これによりクライアント・暗号ゲートウェイ装置間で同一のセッション鍵を共有する（ステップ４）。クライアントは、暗号ゲートウェイとの暗号同期を確立し（ステップ５）、暗号同期確立を契機としてサーバとのセッションを確立する（ステップ６）。これ以降、クライアント・サーバ間のセッションが切断されるまでクライアント・ゲートウェイ装置間の暗号通信が可能である（ステップ７）。

【００１４】なお、ステップ３において、鍵配送センタ１よりセッション鍵を得る場合には、クライアントでもよく、クライアントがセッション鍵を取得すると暗号ゲートウェイ装置に配送することによりセッション鍵を共有することができる。

【００１５】このように、本発明は、サーバにフロントエンドプロセッサとして暗号ゲートウェイ装置を接続し、この暗号ゲートウェイ装置がクライアントからの暗号通信要求を契機として、鍵配送センタにアクセスし、セション鍵を取得し、通信相手であるクライアントにも同じセッション鍵を配送し、セッション鍵を共有することにより、既存のアプリケーションプログラムやハードウェアの更新や、変更等を行わずに、暗号通信を行う。

【００１６】

【実施例】以下、図面と共に本発明の実施例を詳細に説明する。

【００１７】図３は、本発明のシステム全体図である。同図に示す通信システムは、ネットワーク２を介して鍵配送センタ１と複数のクライアント３、暗号ゲートウェイ４が接続され、暗号ゲートウェイ装置４にサーバ５が接続されている。また、クライアント３のフロントエンドとして暗号ゲートウェイ装置４が接続されることも考えられるが、本実施例では、暗号ゲートウェイ装置４は、サーバのフロントエンドとして接続されていることを前提とする。

【００１８】以下、コネクション型のプロトコルを使用してパケット交換網を介して、通信を行うＴＣＰ／ＩＰ・ＬＡＮ（Transmission Contorol Protocol, Internet Protocol, Local area network）を例にとり、詳細に説明する。

【００１９】図４は、本発明の一実施例のシステム構成を示す。同図における通信システムは、鍵配送センタ１、ネットワーク２、クライアント３、暗号ゲートウェイ装置４及びサーバ５より構成される。

【００２０】鍵配送センタ１は、セッション鍵を生成して、暗号ゲートウェイ装置４に送信する。ネットワーク２は、クライアント３とサーバ５間、鍵配送センタ１と暗号ゲートウェイ装置４間、クライアント３と暗号ゲートウェイ装置４間でセッションを確立し、通信を行う。クライアント３及びサーバ５は、パケットのやり取りを行うことにより通信する。暗号ゲートウェイ装置４は、クライアント３とサーバ５間でやりとりするパケットを暗号化／復号する。

【００２１】クライアント３は、暗号ゲートウェイ装置４に暗号通信を要求し、セッション鍵を取得するセッション鍵配送部３１と、セッション鍵配送部３１から受け取ったセッション鍵をセッション毎に管理する鍵管理部３２と、クライアント３と暗号ゲートウェイ装置４間で暗号通信の同期を確立する暗号同期確立部３３と、暗号同期確立部３３から暗号同期確立完了信号を受け取ってサーバ５とのセッションを確立するセッション制御部３４と、アプリケーション（ＡＰ）から受け取ったデータをサーバ５から受け取った暗号化されたパケットを復号する暗号化／復号部３５と、ネットワーク２から（へ）暗号化されたパケットを受信（送信）する送信／受信部３６から構成される。

【００２２】また、暗号ゲートウェイ装置４は、クライアント３からの暗号通信の要求を受け取り、鍵配送セン

タ１からセッション鍵を取得し、クライアント３に配送するセッション鍵配送部４１と、セッション鍵配送部４１から受け取ったセッション鍵をセッション毎に管理する鍵管理部４２と、クライアント３と暗号ゲートウェイ装置４間で暗号通信の同期を確立する暗号同期確立部４３と、クライアント３あるいは、サーバ５から（へ）パケットを受信（送信）する送信／受信部４４と、送信／受信部４４から受け取ったパケットのＩＰヘッダ及びＴＣＰヘッダから送信元ＩＰアドレス、送信元ポート番号、送信先ＩＰアドレス及び送信先ポート番号を取り出し、セッション番号を識別するセッション番号をキーとして鍵管理部４２からセッション鍵を取得し、当該セッション鍵がサーバ５宛のパケットのものであれば、当該パケットを復号し、一方、当該セッション鍵がクライアント３宛のパケットであれば、当該パケットを暗号化する暗号化／復号部４６から構成されている。

【００２３】図５は、ＴＣＰ／ＩＰ・ＬＡＮで使用するプロトコルをＯＳＩの参照モデルに準拠して記述している。データリンクレイヤは、ＭＡＣ（Media Access Control）プロトコル、ネットワークレイヤは、ＩＰ（Internet protocol）、トランスポートレイヤはＴＣＰ(Transmit Control Protocol）で実現されており、ＡＰは、ＴＣＰレイヤ間でセッションを確立する。

【００２４】図６は、ＴＣＰ／ＩＰ・ＬＡＮに接続されたクライアント・サーバ間で通信する際に使用するパケット・フォーマットを示す。パケットは、ＭＡＣヘッダ（ＭＡＣ＿Ｈ），ＩＰヘッダ（ＩＰ＿Ｈ）及びＴＣＰヘッダ（ＴＣＰ＿Ｈ）からなるヘッダと、ＡＰデータ及びパケット全体のフレーム・チェック・シーケンス（ＦＣＳ）から構成される。ＡＰデータに暗号をかけることにより、ＩＰルータを介したネットワークを使用して通信を行うことができる。なお、送信側のＩＰアドレス（ＩＰヘッダに規定）及び、ポート番号（ＴＣＰヘッダに規定）と受信側のＩＰアドレス及びポート番号により、クライアント・サーバ間のセッションが一意に決定される。

【００２５】暗号ゲートウェイ４のセッション識別部４５は、送信／受信部４４を介して受け取った図６に示すＴＣＰヘッダ、ＩＣヘッダから送信元（クライアント）ＩＰアドレス、送信元（クライアント）のポート番号、送信先ＩＰアドレス、送信先ポート番号よりセッション番号を得る。セッション識別部４５により得られたセッション番号に基づいて鍵管理部４２から対応するセッション鍵を取得し、当該暗号ゲートウェイ装置４に接続されているサーバ宛のパケットであれば、暗号化／復号部４６において取得したセッション鍵により復号し、サーバ５に対して非暗号化通信を行う。

【００２６】図７は、ＴＣＰヘッダのフォーマットを示す。同図において、“＿”部分は、本発明に直接関係がないため、ここでは説明を省略する。同図に示すＴＣＰ

ヘッダは６フレームからなり、第１フレームには、ソースポート番号“ＳＲＣ＿ＰＯＲＴ”及び送信先ポート番号“ＤＳＴ＿ＰＯＲＴ”が設定される。６フレーム目にはオプションが設定され、７フレーム目より任意のアプリケーションデータが設定される。

【００２７】クライアント３からの暗号ゲートウェイ装置４に対する暗号通信の要求方法として、

①暗号ゲートウェイ装置４の特定ポート番号に対するセッション確立

②オプションを利用したメッセージ（暗号通信要求）の送信

③ＡＰデータを利用したメッセージ（暗号通信要求）の送信

がある。

【００２８】図８は、本発明の一実施例の鍵配送手順を示すシーケンスチャートである。同図に基づいて以下にセッション鍵の配送の手順を説明する。なお、クライアント３及び暗号ゲートウェイ装置４の暗号鍵K_{c1}及びK_{gw}は、各装置のインストール時に各々装置内部に保持しており、外部からみることができない作りになっている。また、図８において、セッション鍵K_S＝ｄK_{c1}（C_{c1}）：K_Sは、暗号文C_{c1}を暗号鍵K_{c1}で復号した結果である。

【００２９】手順１）クライアント３は、サーバ５とのセッション確立に先立ち、暗号ゲートウェイ装置４とセッションを確立し（ステップ１０１）、暗号ゲートウェイ装置４に暗号通信を要求する。この時、暗号ゲートウェイ装置４にクライアントの識別子ID_{c1}を送信する（ステップ１０２）。

【００３０】手順２）暗号ゲートウェイ装置４は、暗号ゲートウェイ装置４からの通信要求を検出すると、鍵配送センタ１にアクセスし、鍵取得手順（ステップ１０３）（詳しくは図９に示す）により、クライアント３及び暗号ゲートウェイ装置４のそれぞれの暗号鍵（K_{c1}及びK_{gw}）で暗号化されたセッション鍵（C_{c1}及びC_{gw}）を鍵配送センタ１から受信する（ステップ１０４）。

【００３１】手順３）セッション鍵C_{gw}を暗号ゲートウェイ装置４の暗号鍵K_{gw}で復号し、セッション鍵K_Sを取得する（ステップ１０５）。セッション鍵K_Sはサーバ５とのセッションを切断するまで保持する。

【００３２】手順４）暗号ゲートウェイ装置４は、クライアント３に鍵配送センタ１から受信したセッション鍵C_{c1}を送信する（ステップ１０６）。

【００３３】手順５）クライアント３は、暗号ゲートウェイ装置４からセッション鍵C_{c1}を受信する（ステップ１０７）。

【００３４】手順６）クライアント３は、自分の暗号鍵K_{c1}を用いてセッション鍵C_{c1}を復号し、セッション鍵K_Sを取得する（ステップ１０８）。これにより、クライアント３と暗号ゲートウェイ装置４間で同じセッショ

ン鍵を持つこととなる。セッション鍵K_sは、サーバ５とのセッションを切断するまで保持する。

【００３５】手順７）暗号同期確立部３３、４３がクライアント３と暗号ゲートウェイ装置４間で、暗号同期の確立を行う（ステップ１０９）。暗号同期確立が完了すると、クライアント３は、暗号ゲートウェイ装置４とのセッションを切断する（ステップ１１０）。なお、暗号同期の確立方法は、本発明とは直接関係がないので、説明は省略する。

【００３６】手順８）クライアント３はサーバ５とセッションを確立する（ステップ１１１）。

【００３７】手順９）以降、共通のセッション鍵K_sを用いてクライント３と暗号ゲートウェイ装置４間の暗号通信が可能である（ステップ１１２）。

【００３８】手順１０）暗号ゲートウェイ装置４は、クライアント３からサーバ５宛のパケットを受信し、該当するセッション鍵を使用してパケットを復号する（ステップ１１３）。この復号されたパケット（平文のパケット）をサーバ５に送信することにより、暗号ゲートウェイ装置４とサーバ５間で非暗号通信が可能である（ステップ１１４）。

【００３９】また、サーバ５からクライアント３宛のパケットについては、暗号ゲートウェイ装置４において、暗号化され（ステップ１１３’）、暗号化された暗号文にてクライアント３との暗号通信を行う。

【００４０】次に、図９は、本発明の一実施例の暗号ゲートウェイ装置の鍵取得手順を示すシーケンスチャートである。

【００４１】手順１）暗号ゲートウェイ装置４のセッション鍵配送部４１は、鍵配送センタ１にアクセスし、セションを確立する（ステップ２０１）。

【００４２】手順２）暗号ゲートウェイ装置４は、鍵配送センタ１にクライアント３及び暗号ゲートウェイ装置４の識別子ID_{c1}及びID_{gw}を送信する（ステップ２０２）。なお、識別子ID_{c1}及びID_{gw}は装置を識別するための使用するＩＰアドレス或いは、ＭＡＣアドレスである。

【００４３】手順３）鍵配送センタ１は、乱数を発生し、セッション鍵K_sを生成する。さらにクライアント３及び暗号ゲートウェイ装置の暗号鍵K_{c1}及びK_{gw}を識別子ID_{c1}及びID_{gw}に基づいて検索（或いは生成）する。ここで、暗号鍵K_{c1}及びK_{gw}の検索（或いは生成）する方法は、本発明の要点とは、直接関係がないので説明は省略する。

【００４４】検索により暗号鍵K_{c1}及びK_{gw}を取得する場合には、暗号ゲートウェイ装置４の識別子及び暗号鍵を鍵配送センタ１のデータベースに登録する手段が必要であることは言うまでもない。

【００４５】さらに、詳しい暗号鍵K_{c1}及びK_{gw}を生成する方法については、“小柳津、田中『ＵＵＩを利用した鍵配送方式』、信学技報、ＯＦＳ９２－３１”を参照されたい。上記暗号鍵K_{c1}及びK_{gw}を用いて、セッション鍵K_sを暗号化し、暗号文C_{c1}及びC_{gw}を生成する。図９において、$C_{c1}=eK_{c1}(K_s)$：C_{c1}は、平文K_sを暗号鍵K_{c1}で暗号化した結果である（ステップ２０３）。

【００４６】手順４）鍵配送センタ１は、暗号ゲートウェイ装置４に暗号文C_{c1}及びC_{gw}を送信する（ステップ２０４）。

【００４７】手順５）暗号ゲートウェイ装置４のセッション鍵管理部４２は、暗号文C_{c1}及びC_{gw}を受信すると、鍵配送センタ１とのセッションを切断する（ステップ２０５）。

【００４８】ここでは、暗号ゲートウェイ装置４と鍵配送センタ１間は、セッションを確立して通信を行う例を説明したが、ＵＤＰプロトコルを使用するコネクションレス型の通信を使用してもよいし、また、他の通信手段を使用してもよいということはいうまでもない。

【００４９】さらに、本発明は、鍵配送アルゴリズムを特定したものではない。従って、送信するデータの内容（ここでは、識別子ID_{c1}、ID_{gw}、C_{c1}、及びC_{c1}）を変更すれば、相手端末の認証ができることについては“小柳津、田中：『ＵＵＩを利用した鍵配送方式』、信学技報、ＯＦＳ９２－３１”を参照されたい。

【００５０】なお、上記実施例では、暗号ゲートウェイ装置４が鍵配送センタ１よりセッション鍵を取得する場合について説明したが、クライアント３が同様に、鍵配送センタ１より取得し、暗号ゲートウェイ装置４にセッション鍵を配送してもよい。従って、上記図９に示す暗号ゲートウェイ装置４をクライアント３に読み替えればよい。

【００５１】上記の実施例のように、ネットワーク２を介してクライアント・サーバ間の暗号通信を行う場合に、ネットワーク２とサーバ５間に暗号ゲートウェイ装置４を接続し、クライアント３とサーバ５間のセッション確立に先立って、クライアント３から暗号通信要求時に暗号ゲートウェイ装置４が鍵配送センタ１よりセッション鍵を取得し、クライアント３に配送する。これにより、クライアント３・暗号ゲートウェイ装置４間で同一のセッション鍵を共有する。これにより、クライアント３は、暗号ゲートウェイ装置４と暗号同期をとり、これを契機にクライアント３は、サーバ５とのセッションを確立する。この場合、サーバ５とゲートウェイ装置４の通信は、平文通信が行われる。このように、最終的にクライアント３とサーバ５のアプリケーションやハードウェアを変更することなしに、暗号通信が可能となる。

【００５２】本発明は、上記実施例に限定されることなく、暗号ゲートウェイ装置４がサーバ５以外にクライアント３側に接続されてもよく、本発明の範囲を逸脱しない範囲で種々ネットワークを介した接続の変更及び鍵の

11

取得が可能である。

【００５３】

【発明の効果】上述のように、本発明によれば、クライアントとサーバの通信用セッションが確立する前に、サーバと接続されている暗号ゲートウェイ装置がクライアントからの暗号通信要求を受け付け、鍵配送センタにアクセスし、通信に使用するセッション鍵を取得し、通信相手であるクライアントにセッション鍵を配送し、クライアントと暗号ゲートウェイ間で、共通の鍵を共有し、このセッション鍵を用いて、暗号通信を行うため、従来のように既存のアプリケーションやハードウェアを改造する必要がなく、経済化を図ることができる。

【図面の簡単な説明】

【図１】本発明の原理構成図である。

【図２】本発明のシーケンスの概要を示す図である。

【図３】本発明のシステム全体図である。

【図４】本発明の一実施例のシステム構成図である。

【図５】ＴＣＰ／ＩＰ・ＬＡＮで使用するプロトコルを示す図である。

【図６】ＴＣＰ／ＩＰ・ＬＡＮのパケット・フォーマットを示す図である。

【図７】ＴＣＰヘッダのフォーマットである。

【図８】本発明の一実施例のシーケンスチャートである。

【図９】本発明の一実施例の暗号ゲートウェイ装置の鍵取得手順を示すシーケンスチャートである。

【図１０】従来の暗号通信システムの構成図である。

【図１１】従来の暗号通信システムを説明するための図である。

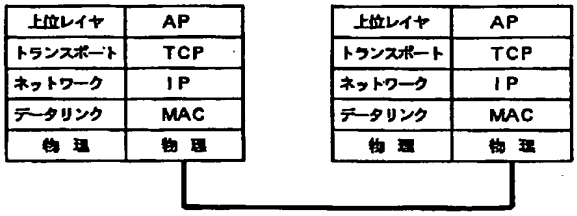
12

【符号の説明】

１　鍵配送センタ
２　ネットワーク
３　クライアント
４　暗号ゲートウェイ装置
５　サーバ
３１　セッション鍵配送部
３２　鍵管理部
３３　暗号同期確立部
３４　セッション制御部
３５　暗号化／復号部
３６　送信／受信部
４１　セッション鍵配送部
４２　鍵管理部
４３　暗号同期確立部
４４　送信／受信部
４５　セッション識別部
４６　暗号化／復号部
１０１　セッション鍵取得手段
１０２　セッション鍵保持手段
１０３　同期確立手段
１０４　第１のセッション確立手段
１０５　クライアントセッション鍵配送手段
１０６　第２のセッション確立手段
１０７　第１のゲートウェイセッション鍵配送手段
１０８　セッション鍵受信手段
１０９　第２のゲートウェイセッション鍵配送手段
１１０　第１の暗号化／復号手段
１１１　第２の暗号化／復号手段

【図５】

（TCP／ＩＰ・LANで使用するプロトコル）



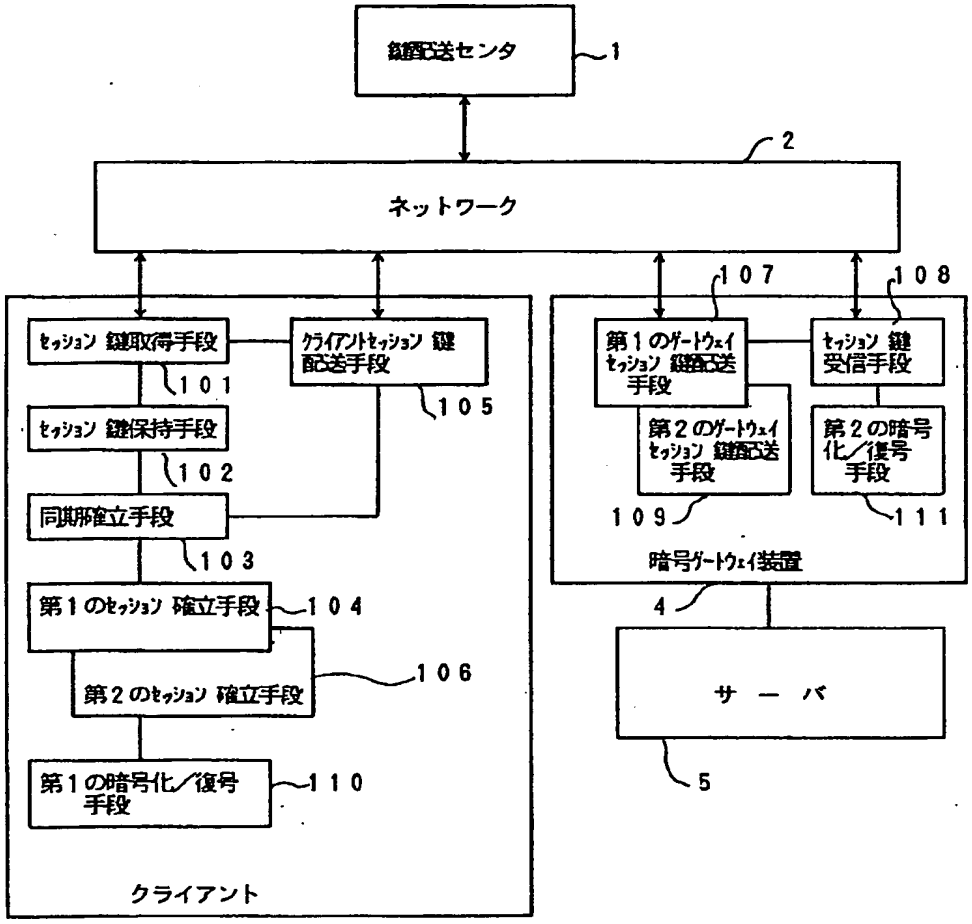
【図６】

（TCP／ＩＰ・LANのパケット・フォーマット）

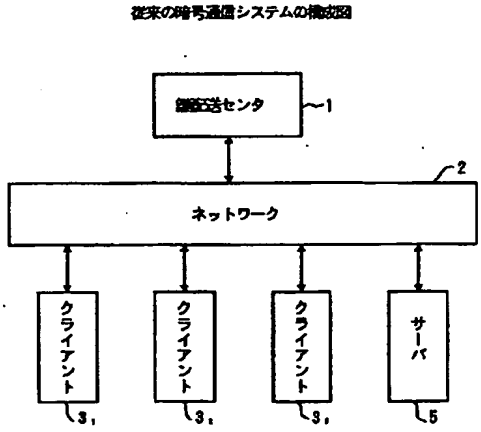
MAC_H：MACヘッダ
IP_H　：IPヘッダ
TCP_H：TCPヘッダ
FCS　：フレーム・チェック・シーケンス
：暗号化領域

【図１】

本発明の原理構成図

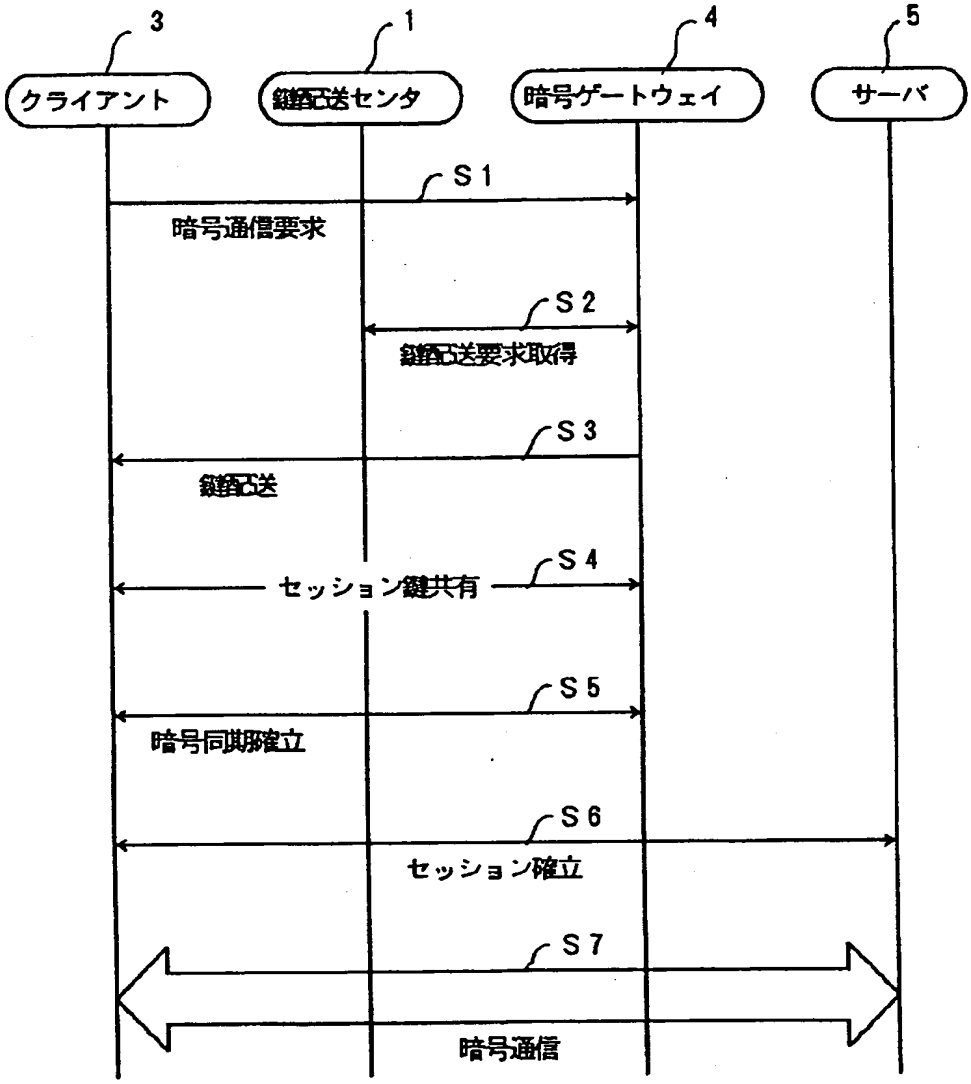


【図１０】



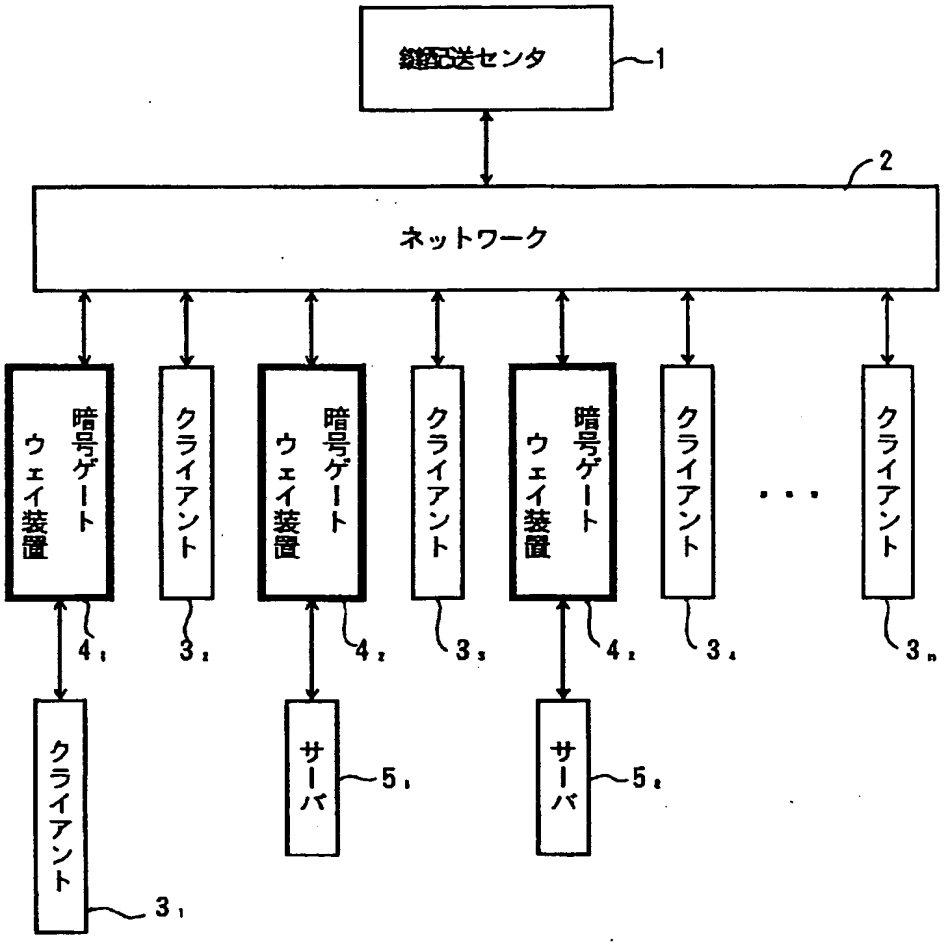
【図２】

本発明のシーケンスの概要を示す図



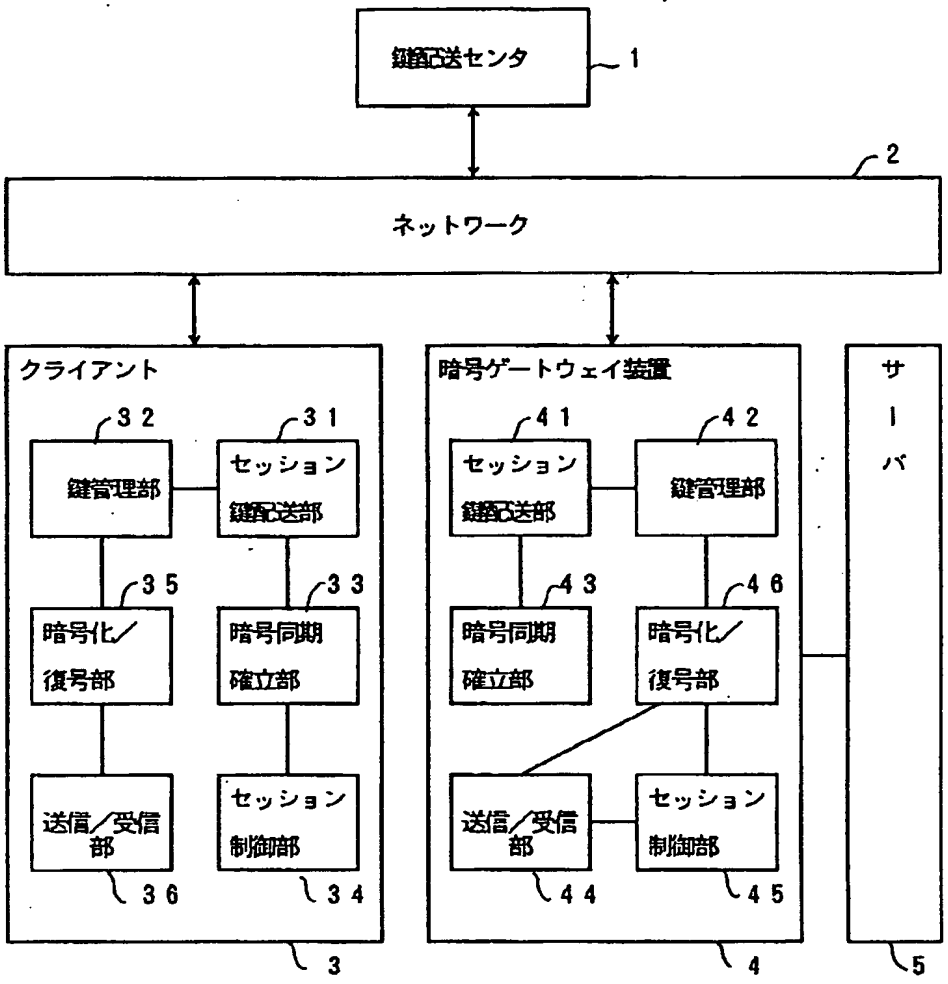
【図３】

本発明のシステム全体図



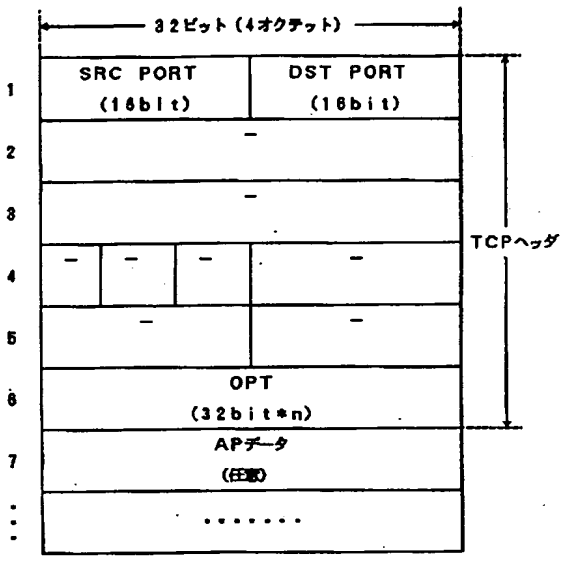
【図４】

本発明の一実施例のシステム構成図



【図７】

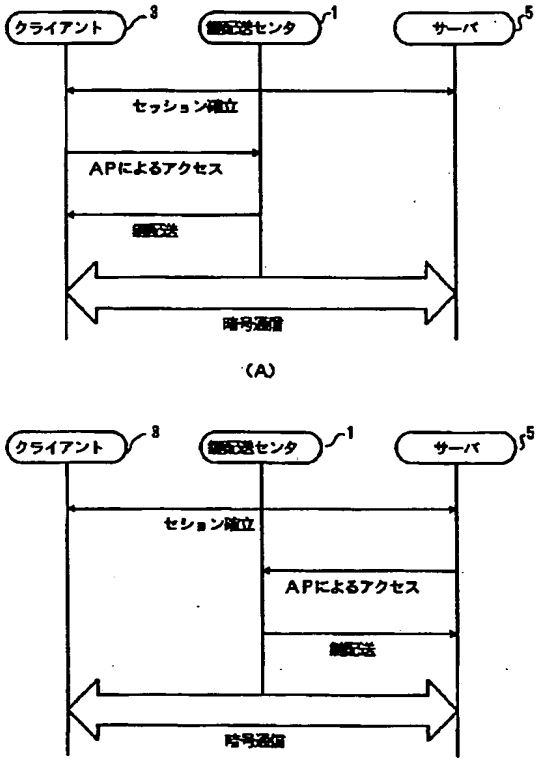
TCPヘッダのフォーマット



SRC PORT：ソース・ポート
DST PORT：デスティネーション・ポート
OPT：オプション

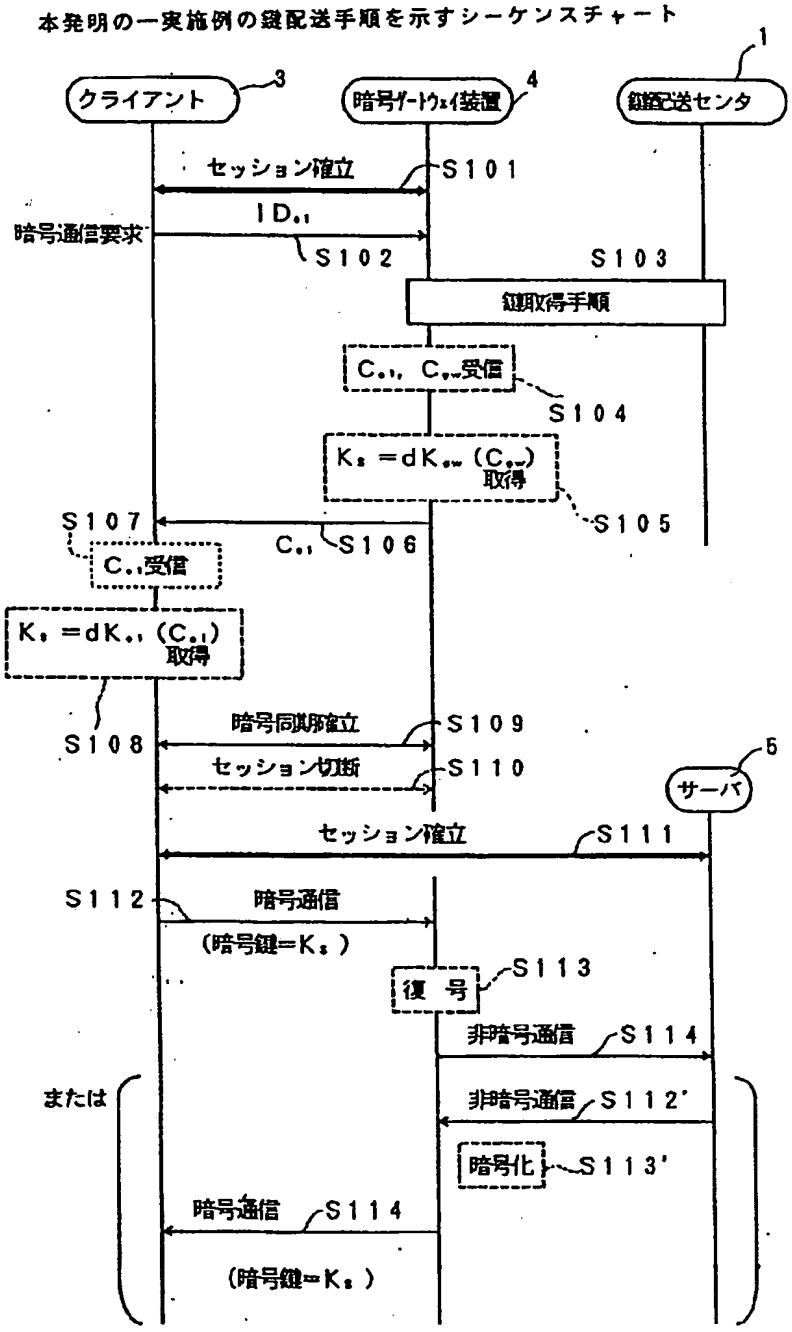
【図１１】

従来の暗号通信システムを説明するための図



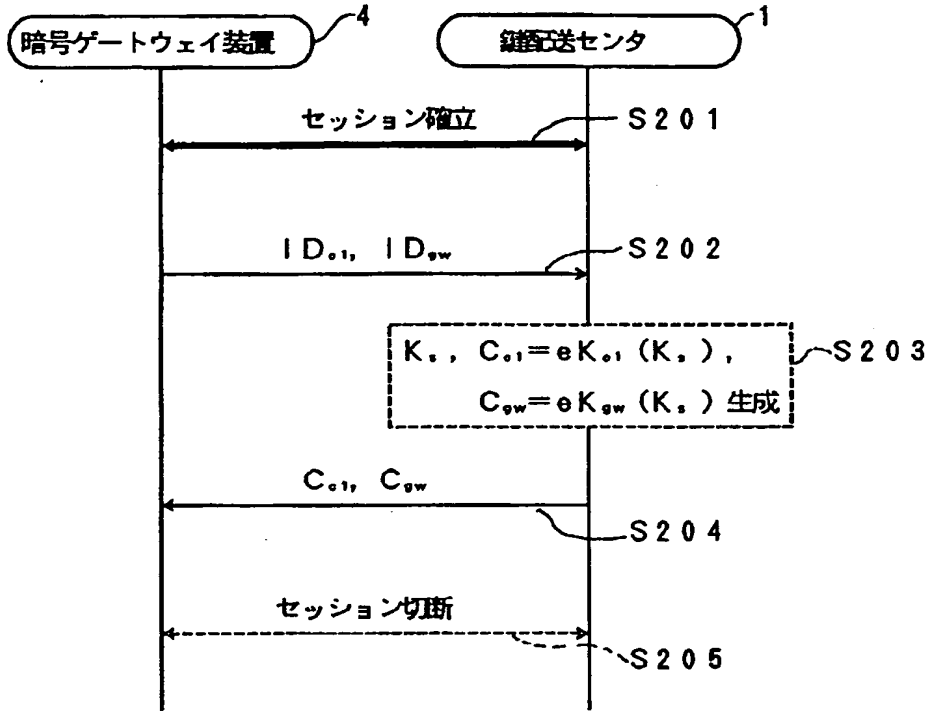
【図８】

本発明の一実施例の鍵配送手順を示すシーケンスチャート



【図９】

（鍵配送センター暗号ゲートウェイ装置間の鍵取得手順）



（注）C。１＝eK。１（K。）：C。１は平文K。を暗号鍵K。１で暗号化した結果である。

フロントページの続き

(56)参考文献　特開　昭63－274242（ＪＰ，Ａ）
特開　平４－179326（ＪＰ，Ａ）
特開　平７－107084（ＪＰ，Ａ）
山口利和，田中清人，田辺克弘，小柳津育郎，ＬＡＮの暗号通信における一方式，電子情報通信学会技術研究報告（ＯＦＳ93－32），日本，社団法人電子情報通信学会，1994年　1月21日，Ｖｏｌ．93，Ｎｏ．435，ｐ．13－18
山口利和，田中清人，田辺克弘，小柳津育郎，ＬＡＮ暗号通信方式の実装と評価，電子情報通信学会技術研究報告（ＯＦＳ93－38），日本，社団法人電子情報通信学会，1994年　3月11日，Ｖｏｌ．93，Ｎｏ．508，ｐ．７－12
山口利和，田中清人，田辺克弘，小柳津育郎，ＬＡＮセキュリティ通信技術－ＴＣＰレイヤにおける通信データの暗号化－，ＮＴＴ　Ｒ＆Ｄ，日本，社団法人電気通信協会，1995年　7月　8日，Ｖｏｌ．44，Ｎｏ．９，ｐｐ．653－660

(58)調査した分野(Int.Cl.⁷，ＤＢ名)
H04L　9/08
H04L　12/28